International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN (P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 4, Aug 2014, 103-120

TRANS STELLAR
• Journal Publications • Research Consultancy

PENETRATION TESTING IN WI-FI NETWORKS

SHORUNKE MUYIWA MUSADDIQ

Department of Mathematics & Computer Science, Elizade University Ilara-Mokin, Ondo State, Nigeria

ABSTRACT

Wi-Fi network connection access points are easily discovered all around us today through the use of any free Wi-Fi discovery tool made available free on the web, also with the aid of common hardware such as laptops that are Wi-Fi enabled. Its usage ranging from private to corporate and public use, has made it a favourable target for attacks by black hat hackers. Unfortunately, most Wi-Fi network users do not see the significance and effectiveness of conducting security audits routinely in order to fortify their network and to detect how weak and vulnerable their Wi-Fi network is to malicious attacks. Although conducting a proper penetration test on a Wi-Fi network can be tasking and quite expensive, but its value cannot be underestimated. Unlike most private users, corporate users often do carry out security audits (i.e. Penetration Tests) so as to protect their web-based assets. This paper looks into the various types of attacks faced by Wi-Fi network users, particularly the private users. The paper further highlight most security weakness encountered on private Wi-Fi network with simple network penetration test conduct. Finally, the papers suggests and propose simple and less expensive countermeasures that Wi-Fi private users can employ to properly secure and improve the quality of performance the Wi-Fi network connection access.

KEYWORDS: Wi-Fi Network, Penetration Test, Security, WEP, WPA, Denial of Service (Dos), WPA2

INTRODUCTION

With the rapid change in global technology in the present day, a paradigm shift from wired/cabled networking in the field of digital information and communication was initiated. For the ease of mobility, cost and flexibility, most digital devices today are now been transformed from being wired to wireless. Wireless networks are excellent compliments to fixed (cabled) networks, but they are not a replacement technology (Matthew Gast 2002).

The transformation of internet access into (wireless), Wi-Fi networks has brought about a significant development in networking, majorly because they complement fixed (cabled) network by providing mobility to users. With the increasing usage of wireless networks, Wi-Fi network users (private & corporate) are now faced with various security issues ranging from malicious attacks and unauthorized access their network database (hacking) to Denial of service attacks. In 2003, the Wi-Fi Alliance in collaboration with the institute of electrical and electronics engineers (IEEE) developed a stronger tolerant Wi-Fi security specification in the form of Wi-Fi protected access (WPA) to address all the known security weakness of Wi-Fi networks provided by the default security mechanism *wired equivalent privacy* (WEP). Although WPA addresses most security flaws in wired equivalent privacy (WEP), a couple of educational research and studies with the academic forte and private information security outfits came out with the result that an attacker or intruder adequately with appropriate tools and techniques, alongside a considerable amount of technical knowledge can potentially gain unauthorized access to a Wi-Fi network despite the network been WPA enabled.

Over the years Wi-Fi network have encountered various attacks such as; ARP Poisoning (Address Resolution Protocol), Man-in-middle attack, Denial of Service attacks (Jamming, sleep deprivation, spoofing) and finally passive attacks such as *war driving*. These amongst other forms of attacks has been the problems faced by Wi-Fi users all around the world. Most private or individual users rely solely on their local firewall provided been provided by their operating system vendor for security. Although these vendors regularly provide security patches for their users by creating security patches updates to mitigate these malicious attacks. Unlike private users, corporate users such as firms, schools, industry, and government setups do not solely rely on localfirewall provided by their operating systems but also use other forms of sophisticated and trusted security tools. Corporate users tend to hold important information in their database, which are mostly confidential and most maintain the integrity of such information. This led to the idea of corporate users recruiting security experts to test and discover various security vulnerabilities on the Wi-Fi / Wireless networks. This paper therefore focuses and evaluates the security vulnerabilities of private users Wi-Fi network that could be as a result of poor or improper system configuration or both on the part of the hardware and software flaws of their network.

Penetration Testing

"Penetration Testing" is a familiar term in today's world in the field of computing / network security; it basically entails the various techniques of evaluating the security strength of a computer system or network by simulating attacks from a malicious source. Wi-Fi networks faces multiple source of attacks with the use of sophisticated tools and well deployed techniques from attackers in order to fully exploit the security vulnerabilities of the network. Various experts in the field of network security have contributed their quota to the subject matter via various media, ranging from articles, journals, books and research test etc. One of the most reliable method of checking the integrity of your Wi-Fi security is through penetration testing (JhoanaCooper 2009). The author stated further in her article why penetration testing in Wi-Fi network is very important for all Wi-Fi network users.

Attacks on Wi-Fi networks and their users have increased tremendously over the years as the use of Wi-Fi services has become more common and popular as compared to its advent. Some of the main reasons for this could be attributed to the fact that malicious attack methods are more sophisticated today and the availability of hacking tools, such as software's are now been made available free on the web. This major factor poses a major threat to Wi-Fi users and puts their data at security risk.

Wi-Fi Security

The major between Wi-Fi and wired networks in terms of security is the access to transmitted data. In Wi-Fi network, data is being transmitted in the air via radio frequency which can be easily accessed with various techniques and tools, made available today in the market. While wired network Transmitted data can only be accessed via the network devices being used for the network data transmission. Wi-Fi networks have been noted to be prone to more attacks and less secure in terms of security than wired networks, this is majorly because Wi-Fi networks transmit data into the air, which gives any potential passer-by with-in the proximity and of the right knowledge, technique and tools the liberty to intercept these traffic transmissions. Network security experts have noted that the most challenging setback being faced by Wi-Fi networks is the issue of security. Although Wi-Fi network users are prone to various malicious attacks, these security risks can be addressed and mitigated by reasonable security precautions in which one the major ways of doing this is by conducting penetration tests on the network.

Wi-Fi Security Mechanisms and Protocols

Wired Equivalent Privacy (WEP) is known to be the initial default security specification standard provided for wireless networks. As time went on various security weaknesses were discovered and identified by cryptanalysts in the security specification standard which thereby led to the invention of a new security system scheme by the Wi-Fi Alliance called WPA (Wi-Fi Protected Access) in 2003. Later on in the year 2004, the full IEEE 802.11 security specification standard (WPA2) was introduced.

Wired Equivalent Privacy (WEP) Mechanism

WEP was intended to provide a security scheme for Wi-Fi networks and its users that are equivalent to that of a wired network. WEP was not developed with the intention to provide a level of security superior to or higher than that a wired network, rather equivalent to it. Hence the name of the protocol was been generated "Wireless Equivalent Privacy". Wi-Fi users became less secure due that fact WEP keys could be easily cracked within a short time frame. Most private users today still make use of WEP to protect intruders from gaining access into their Wi-Fi network connection, but can they be blamed for this? According to a report from the BBC news, findings have it that most Wi-Fi network vendors in the United Kingdom such as BT, which is one Britain's leading and largest Wi-Fi network provider supply intending Wi-Fi users with WEP pre-con.ured routers rather than WPA (Wi-Fi protected Access) compatible routers. Attackers can easily penetrate into WEP protected Wi-Fi networks with the aid of several tools made available online e.g. Airsnort-ng, thereby gaining full access into networks valuable data such asPasswords, vital information, confidential information and in some cases download illegal pornographic material with the Wi-Fi connection. Bearing in mind the implication of such acts to the administrator or owner of the Wi-Fi network access that may involve legal issues requiring law enforcement agents like the police force to seize the user’s desktop or laptop for forensic analysis and also implicate the user’s name. Although most Wi-Fi network users, majorly private users are mostly ignorant of the security implication of using WEP cryptographic keys to secure their network and also the importance of conducting a security audit (penetration test) every once in a while in order to protect their network connection access. This is majorly due to the fact that most of these private users are not properly oriented about the risk and implications involved in leaving their Wi-Fi connections unprotected or using WEP as their security standard. Personally I think a particular body or outfit should be setup by the government for such awareness or possibly vendors should be imposed to provide better security standards or better still educate their clients and customers about these security issues.

Wi-Fi Protected Access (WPA) Protocol

Wi-Fi Protected Access (WPA) was the immediate solution for Wired Equivalent Privacy (WEP), WEP received a great deal of negative criticism due to various technical failures in the protocol. So, the standard bodies and industry organizations have been spending a great deal of time and money on developing and deploying nextgeneration solutions that address growing wireless network security problems.

Taking into consideration the vulnerabilities and flaws in WEP, the Wi-Fi (Wireless Fidelity) Alliance, has created the Wi-Fi Protected Access (WPA) standard which is a subset of the 802.11 draft. WPA has brought about majorly three advancement and improvement over WEP security protocol, they are; improved data encryption, user authentication, and integrity. Corporate Wi-Fi network users are the most type of users discovered to employ this better form of Wi-Fi security mechanism. Although WPA did reduce intrusion attacks on Wi-Fi networks by the provision of temporary keyintegrity

protocol (TKIP) that was much needed in Wi-Fi security. Wi-Fi users no doubt are more secure a bit with the advent of WPA security protocol, but this security protocols over the years has been discovered to have its own flaws, some of these flaws include;

- If an attacker successfully by passes one layer of the Wi-Fi security, the attacker can potentially cause denial of service attack to the Wi-Fi network.
- Another major flaw been encountered with WPA is the use of Pre-Shared Keys, in which most private users and some cooperate users that cannot afford to use separate servers for authentication and full 802.1x key infrastructure, this process occurs during "handshaking" i.e. the exchange of information that are used to generate data encryption keys for wireless sessions. This process allows the attacker to sniff the Wi-Fi network traffic in transit between the access point and the Wi-Fi workstation, and then use a specialized sophisticated software programs to predict the encryption key.

Wi-Fi Protected Access 2 (WPA2) Protocol

There is no doubt the Wi-Fi protected access (WPA) is a better Wi-Fi network security protocol than WEP, since it addressed major flaws and weakness found in the previous security protocol, also because its backward to compatible with all the existing Wi-Fi devices and equipment. However WPA is still seen by some Wi-Fi security experts to be vulnerable to some extent, and this is solely attributed to the fact that WPA relies on the (Rivest Cipher 4) RC4 encryption algorithm and TKIP (Temporary Key Integrity Protocol). In order to finally address this security flaws and weaknesses encountered in the previous security system protocols, the Wi-Fi security standard committee decided to design a security system from the scratch. This new high tech security system is known as WPA2 by the Wi-Fi Alliance.WPA2 uses the Robust Security Network (RSN) concept, with the use of WPA2 the Wi-Fi devices or equipment are required to support the additional capabilities been made available on WPA2. This basically will require new Wi-Fi hardware and software drivers, thereby making a complete compliant WPA2 Wi-Fi network incompatible with existing WEP devices and equipment. In the transitional period both RSN and WEP equipment will be supported, (in fact WPA/TKIP was a solution designed to make use of older equipment) but in the longer term WEP devices will be phased out. 802.11i allows for various networks Implementations and can use TKIP, but by default RSN uses AES (Advanced Encryption Standard) and CCMP (Counter Mode CBC MAC Protocol) and it is this, which provides for a stronger, scalable solution.

Analysing Wi-Fi Networks Security

WPA2 is presently believed to be the most secured Wi-Fi security standard and protocol, although even the cooperate Wi-Fi network users who spend a great deal of money and time to secure their Wi-Fi network security cannot really be guaranteed 100% that their network’s security is unbreakable. Personally I deem WPA2 security standard not fully providing the full solution to the security vulnerabilities encountered by Wi-Fi network users, most especially the private home users and small-scale business users for quite a few reasons; WPA2 security standard are mostly implemented by corporate users majorly because they are the only ones who can afford to employ these sophisticated and expensive security mechanism. Private home users who are intending to upgraded or ratify their Wi-Fi network security protocol find it tedious and expensive because they have to install new hardware and software drivers for WPA2 to be fully compliant on their Wi-Fi network because it is not backward compatible with the existing Wi-Fi devices on the Wi-Fi network which may be employing the security mechanism of WEP or WPA security protocol. Irrespective of security mechanism standard

been employed by Wi-Fi network users the major issues they all need to address are securing and maintaining their network connections. In conclusion it all falls back to what measures are been employed by Wi-Fi users to secure their network, how secure is the measure they've employed? Also if it is well protected and secured, how often do they maintain the security on the network? Activities like routine security audits, Penetration tests are vital for all Wi-Fi network users and are essential in order to patch any security vulnerability or vulnerabilities been discovered on the network. Technology as known by all is dynamic, therefore periodically newer threats and techniques would be designed and implemented by attackers and the only way to mitigate such threats and attacks is to carry out penetration tests once in a while to know the security state of one's Wi-Fi network.

Types of Attacks on Wi-Fi Networks

Wi-Fi networks encounter various forms of malicious attacks, but these are classified basically into two categories. They are; Passive attack and active attack.

Passive Attacks

Passive attacks on Wi-Fi networks is the preparatory phase of an attack, in order words it's the footprinting phase of the network i.e. when attackers seek to gather information about the targeted network prior to the attack launch on the network. Passive attacks on Wi-Fi networks in most cases are not detrimental attacks; this form of attack is simply the process of an attacker eavesdropping or monitoring the network traffic flow or information being transmitted from the network. Passive attack is also known as "interception", this attack is very common on Wi-Fi networks, yet quite difficult to detect and this is solely because most passive attacks do not alter the traffic flow nor the data been deduced from the network system. The only major threat being posed by this attack is the interference in privacy and anonymity of communication, and this is solely because information being obtained from the traffic flow such as; routing information can show the relationship between nodes (addressable devices attached to the network and that can recognize, process, and forward data transmission). Such information can be used for a malicious attack later on the network. There are various types of passive attacks, but the prevalent types of passive attacks on Wi-Fi networks are as follows, war driving, eavesdropping, and traffic sniffing.

War Driving: War driving is simply the act of an individual or group of persons in a moving vehicle searching for active Wi-Fi wireless network access points. Over the years, controversies over war driving being illegal or legal have been a major point of discussion. Most people in the war driving community consider war driving as educational in nature. Although it is also worth noting that war driving is actually not illegal due to the fact that most Wi-Fi network frequency broadcast are being transmitted in public places and thereby makes any legal or connection restriction to public users ofthat location. This makes protecting a Wi-Fi network from passive attacks more difficult. Although in a situation whereby the network administrator or owner of a network notice a car been parked on private property, he or she has the right to ask the vehicle owner(s) to leave or be charged for trespassing on a private property.

The legal implication on such accusation in most cases is limited, Only if it could be proofed that the war driver was actively attempting to crack any encryption been set in place on the Wi-Fi network or interfering and analysing Wi-Fi traffic with the malicious intent to cause some havoc on the network would he or she be susceptible to being charged with a data related crime, but this would also depend on the country which the activity occurred. Several software are being made available online free for war driving enthusiasts, the most used amongst these software is the netstumbler

"www.netstumbler.com". The netstumbler is a freeware program that runs on Wi-Fi adapters, it is a rich product that provides information about Wi-Fi surveys. Netstumbler is not only used for my malicious purpose only but also could help Wi-Fi administrators in performing other useful functions such as,

- Verifying if the Wi-Fi network is been setup /configured properly
- Helps in finding locations with poor network coverage on ones Wi-Fi
- Detecting unauthorized access into one's Wi-Fi network
- Detecting other Wi-Fi network within one's proximity that might be causing interference on one's Wi-Fi network

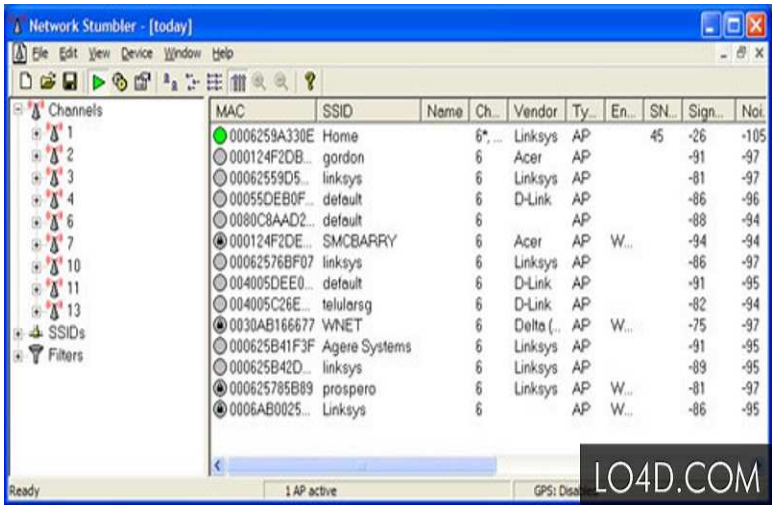

Figure: 1

The. figure 1 shows a typical screen shot interface of a live session of the netstumbler. Netstumbler shows the information on the Service Set Identifier (SSID), the channel, and the manufacturer of the Wi-Fi AP. There are a few things that are particularly noteworthy about this session. The first is that a couple of APs (APs are half-duplex devices and work just like other half-duplex devices, such as hubs and repeaters) are still configured with the default SSID supplied by the manufacturer, which should always be changed to a non-default value upon set up and configuration. Another is that at least one network uses a SSID that may provide a clue about the entity that has implemented it; again this is not a good practice when configuring SSIDs. It is also visible that the networks have implemented WEP.

Eavesdropping: This is another major form of passive attack common on Wi-Fi network. This form of attack involves an attacker monitoring all data/traffic passing through a node in the network. Although in some cases this might be legitimate, this occurs in a situation of a penetration test or the network administrator trying to monitor inappropriate communication between parties in the network. This is majorly because most network communication of Wi-Fi network are in unsecured format or clear text, which aid attackers in gaining access to data path within the network and thereby eavesdrop or intercept the network traffic.

Traffic Sniffing: Wi-Fi traffic sniffing entails the attacker/intruder to be in close proximity of the targeted Wi-Fi traffic. This is an estimated range of about 300 feet, although newly developed sophisticated wireless equipment is capable of delivering signals much further. This allows intruders to conduct their attacks from a farther distance. If the intruder is able to sniff out Wi-Fi traffic, it is also possible that they can insert malicious source codes into the traffic connection.

Which gives them a full control over the network after the successful deployment of this attack. Sniffer is the major application device used in Wi-Fi network that can monitor, capture and read network packets. Attackers use the sniffer to read the network's communication and analyse it to collect necessary information to gain access into the network. Vulnerable network protocols that are often sniffed by attackers for password include; TELNET, IMAP, and POP. Sniffers normally operate by placing all the collected information been sniffed from the network traffic into a log file, although the newer models simply unlink themselves, log files and send logged data to collectors (attacker) in ICMP packets.

Active Attacks

Active attack is the next stage involved mostly after any form of passive attack, all significant information/data been successfully collected from the passive stage of attacks are been deployed at this stage. There are potentially several forms of active attacks on Wi-Fi networks, these includes attacks such as man in the middle attack, Denial of service of attacks, Jamming attack, Spoofing attack, Sleep deprivation attack, ARP poisoning, Masquerading, and Brute force attacks.

Spoofing Attack: Due of the nature of Wi-Fi networks and the flaws of wireless equivalent privacy (WEP), unauthorized access and spoofing are the most common form of attacks encountered on Wi-Fi networks. Spoofing occurs when an attacker is able to use an unauthorized station to impersonate an authorized station on a wireless network. A major way of preventing Wi-Fi network against such an unauthorized access is to use MAC filtering to allow only clients that possess valid MAC addresses access to the Wi-Fi network. The list of permitted MAC addresses can be configured on the AP, or it may be configured on a RADIUS server that the AP communicates with. Although, irrespective of the method been used to implement MAC filtering, it is a relatively easy matter to change the MAC address of a Wi-Fi network device through the software to impersonate a valid station. In Windows, this is accomplished with a simple edit of the registry, in UNIX through a root shell command. MAC addresses are sent in the clear on wireless networks, so it is also a relatively easy matter to discover authorized addresses.

Man-in-the Middle Attack: The Attacker in this situation inserts itself into the communication and becomes a proxy (software to bypass firewalls). The man-in-the middle attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker divides the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, as shown in the diagram below, Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.

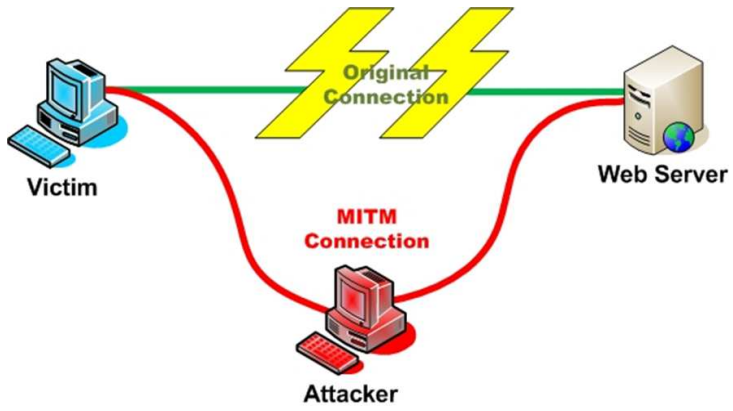

Figure: 2.0

Sleep Deprivation Attack: This form of attack is also a common type of attack on Wi-Fi networks, Attackers simply consumes resources of the devices on the Wi-Fi network. Resources such as the bandwidth, CPU, and power of these devices are usually consumed, and this usually possible because of the power limitation on these Wi-Fi devices which prevent functions such as stand-by mode or system hibernation. This resource consumption attacks ranges from:

- **Malignant Attack**: Executable file is created or existing code is modified to Increase power consumption (e.g. infinite loop)
- **Service Request Attack:** This attack increases the power consumption of the device by engaging the device in servicing invalid network requests (e.g. repeatedly making network requests like telnet, or web requests to device under attack and draining battery power.
- **Benign Power Attack:** The Attacker requests the device to execute a valid, but energy hungry task that drains the power of the device at a fast pace.

ARP Poisoning: (Address Resolution Protocol) is also known as ARP Spoofing. The Address protocol permits Wi-Fi devices that use transmission control protocol/ Internet protocol (TCP/IP) to recognize which other devices on the network possess which IP address. Inorder words ARP broadcasts a request to identify which particular host that is using a certain IP address. The host in question receives that message and acknowledges it, and the originating computer stores the responding computer's MAC address in its cache, knowing that further transmission to that host won't require any further IP address discovery. The Attacker thereby forges a fake ARP address from the network. This is acquirable majorly because it is possible for the attacker to update a host's ARP cache with fake information via the spoofed ARP replies. Attackers in most cases usually then corrupts the directly connected host's ARP cache inorder to finally take over the victim's host IP address. Some of the major tools used for ARP Poisoning are;

- ARP Poison is a UNIX Command-line tool that can be used to create spoofed ARP packets
- Ettercap can be used for filtering, hijacking, poisoning, sniffing, including SSH v.1 sniffing (transparent attack).
- Dsniff can be used for poisoning, sniffing, including SSH v.1 sniffing (proxy attack)
- Parasite is a daemon used to watch a WI-FI network for ARP requests and automatically send spoofed ARP replies.

Masquerading: is another major attack being experienced on Wi-Fi network especially at the network layer. The masquerade attack is such an attack whereby an attacker tries to access a computer pretending to have an authorized user identity such as a network administrator. Masquerading could also be performed at the passive stage of a Wi-Fi network attack, since it's also a form of footprinting on a network. One of the major techniques used in masquerading is “phishing”. Phishing is a familiar term in the present day of computer security; this is simply the act of attackers sending fraudulent mails that looks legitimate with the intent to gather personal and financial information from the recipients. Sensitive information's such as passwords, usernames, and credit card details are usually major attacks been experienced by Wi-Fi network users. Attackers use several numbers of different social engineering techniques to trick Wi-Fi users in providing this personal information.

Denial of Service Attacks: Denial of service attacks or distributed denial of service attack is a form attack on Wi-Fi networks in which a legitimate Wi-Fi user(s) are being deprived of the services of a resource that they are entitled to.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

- Attempts to flood a network, thereby preventing traffic network
- Attempts to disrupt connections between two Wi-Fi devices, thereby preventing access to service or a particular resource.
- Attempts to disrupt service to a specific Wi-Fi device or user
- Attempts to prevent a particular user from accessing a particular service.

Also denial of service attacks is aimed at different services and also in different forms and techniques. They are as follows;

- Usage of scarce, limited, or non-renewable resources
- Damage or alteration of configuration information/data
- Physical destruction or alteration of the network components.

In most cases a denial of service attack usually does not result in the theft of information or other security alteration, loss, or damage, it can cost the target (Wi-Fi user) a great amount of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial of service attackcan also alter and destroy programming and files in affected computer systems. In some cases, denials of service attacks have made many Wi-Fi users unable to access the web and also other Internet related resources; some major types of denial of service attacks are:

SYN Attacks: Whenever a new session is initiated between the Transport Control Program (TCP) client and server in a Wi-Fi network, a very small buffer space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This renders the first packet in the buffer so that other, legitimate connection requests can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these bogus connection requests is to make it difficult for legitimate requests for a session to get established.

Buffer Overflow: This is the most common type of denial of service attack; it basically entails sending more traffic to the Wi-Fi network address than the programmers who designed the data buffers anticipated someone might send. Most attackers are usually aware that the target system has a weakness that can be exploited or they simply try the attack in case it might work. A few of the better-known attacks based on the buffer characteristics of a program or system include;

- Sending e-mail messages that have attachments with 256-character file names to Netscape and Microsoft mail programs
- Sending oversized Internet Control Message Protocol ICMP Packets (this is also known as the Packet Internet or Inter-Network Groper (ping) of death
- Sending to a user of the Pine e-mail programme a message with a "From" address larger than 256 characters.

Smurf Attack: The attacker in this situation sends a forged IP ping echo packets to broadcast addresses of vulnerable Wi-Fi networks with fake source address directly to the victim of the attack. All the system devices on the network reply to the victim with IP echo replies. This is in-return drastically consumes the bandwidth available to the victims Wi-Fi network.

Teardrop Attack: This form of denial of service attack exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash and thereby causing the target victim a great loss of service and time.

Wi-Fi Network Security and Wi-Fi Network Users

A recent German newspaper publication had a statement that Wi-Fi network users in the country could be fined for leaving their Wi-Fi network connection open, according to a new court ruling in Karlsruhe. An incident about a musician whose work had been illegally downloaded over a user's Wi-Fi connection. The user (owner of the Wi-Fi network) who was on a holiday at the time and had documents to prove it, but failed to password (secure) his Wi-Fi connection, which gave any passer-by or person or nearby the opportunity to perform any unscrupulous activity on the web via theopen Wi-Fi network connection. The court ruling stated: "Private users are obligated to check whether their wireless connection is adequately secured to the danger of unauthorized third parties abusing it to commit copyright violation." The verdict was fined €100, which is rather paltry, but probably more than an innocent user with no clue about network security deserves. The musician did not find the Wi-Fi network owner guilty of copyright infringement over the original accusations, but the court believed that some degree of responsibility is needed for third-party misuse of an unsecure connection. Meanwhile the person who actually illegally downloaded the music files is probably somewhere presently with his iPod plugged in and a big fat grin on his face.

Not everyone today know quite a handful about technology and its rapid change. Most people find the court ruling on the Wi-Fi network owner harsh or outwardly wrong, it's like leaving one's front door open and an intruder enters and commits a crime. I personally think no one would be so careless to leave their front door open knowing the implications, so therefore Wi-Fi users should be more careful with their network security. Most Wi-Fi users, mostly private users underestimate the risk in leaving their Wi-Fi network connection unsecured, and even when it's secured it is not properly encrypted i.e. password. These Wi-Fi users usually rely on the security been made available on their Wi-Fi devices such as anti-virus programs, which in most cases cannot tackle all the various forms on attacks on their network. Although some Wi-Fi users such as cooperate users protect their Wi-Fi network with the aid of several techniques and precautions via routine security audits such as penetration tests but not all Wi-Fi users do.

The Act of Penetration Testing

Penetration Testing could be describe as the process of actively exploiting apparent weaknesses and flaws in a network in an attempt to discover security vulnerabilities on the network, and to reveal otherpotential weaknesses on the network. Penetration test provides Wi-Fi network users an invaluable and compelling insight assessment of how their Wi-Fi network security is been seen from outside their domain. A well-executed penetration test shows that security

vulnerabilities do exist and that network intrusion is possible, most importantly they provide a blueprint on how to remedy or start a protection security patch plan. A penetration test simulates covert and malicious network attack activities in order to note specific exploitable security flaws and weaknesses and to expose potential gateways to significant and confidential data, in which if it eventually becomes accessible to an attacker, it could alter the integrity of such data and also pose a great risk and liability loss to the individual user or organization. Qualified security expert consultants conduct penetration tests; basically their main function is they attempt to gain access to their client's online assets and resources via the client's system network server, and work station (desktop(s)) either through the internal or external perspective in such a manner an attacker would. The outcome of these tests by the penetration tester would clearly state he security issues and recommendations and also create a compelling for the individual owner of the network or the entire management team of the organization to support and adhere to a security program. In recent years penetration tests have proven to be a major way of limiting attacks been experienced on Wi-Fi networks, according to report from Internet Security Systems 2001 "A penetration test by a trusted provider offers an excellent means by which an organization can baseline its current security posture, identify threat and security weakness, and start implementing remediation strategies. By identifying risk exposure and highlighting what resources are needed to correct them, penetration test provide not only the basis for a security action plan, but also the compelling events, due diligence and partner interface protocols necessary to establish information security as a key corporative initiative.

Reasons for Penetration Test

According to a tutorial guide by Punnet Mehta 2010, "Penetration Test Guide" which stated several genuine reasons why penetration test is essential and important for all network users both Wi-Fi network and LAN.

- A penetration test helps both private and corporate users to understand their current security posture by identifying gaps and vulnerabilities in security. This enables these users to develop an action plan tominimize the threat of attack or misuse.
- A well-documented penetration test result helps network administrators, most especially the cooperate users, in creating a strong business case to justify a needed increase in the security budget or make the security message heard at the executive level.
- Security is not a single point solution, but a process that requires due diligence. Security measures need to be examined on a regular basis to discover new threats. A penetration test and an unbiased security analysis enable organizations to focus internal security resources where they are needed most. In addition, the independent security audits are rapidly becoming a requirement for obtaining cyber-security insurance.
- Meeting regulatory and legislative requirements are a must for conducting businesses today. Penetration testing tools help cooperate Wi-Fi users meet these regulatory compliances.
- One of the core objectives of an e-business initiative is to enable close working with strategic partners, suppliers, customers and others upon whom the e-business depends. To accomplish this goal, organizations sometimes allow partners, suppliers, B2B exchanges, customers and other trusted connections into their networks. A well-executed penetration test and security audits help organizations find the weakest links in this complex structure and ensure that all connected entities have a standard baseline for security.

- Once security practices and infrastructure is in place, a penetration test provides critical validation feedback between business initiatives and a security framework that allows for successful implementation at minimal risk.

Penetration Test in Wi-Fi Network

Wi-Fi networks connection usage, either for corporate outfit network infrastructure or for private home use, is prone to more security attacks and exposures that are much more threatening than cabled (wired) network attacks. Since, the only boundary Wi-Fi networks know are their signals, it is relatively more easier for attackers to identify Wi-Fi network connections by simply "driving" or walking within the proximity with their wireless network equipment, i.e. war driving. Immediately an open Wi-Fi access point is discovered, the intruder (war driver) usually maps it, so at the end he would have a map of access points with their properties (SSID, WEP, MAC etc.). The main aim of Wi-Fi network penetration testing is basically to identify security vulnerabilities or weakness in the design, implementation or operation of the client's/Users Wi-Fi network. Furthermore Wi-Fi penetration test will also attempt in the access of the Wi-Fi network environment and the configuration of the Wi-Fi infrastructure as well as the other Wi-Fi devices that are connected to it. The test will also involve the test of the strength of the security been deployed already on the Wi-Fi network, thus this will include the assessment of the encryption and authentication control and also a Wi-Fi intrusion detection test to detect rogue access point that masquerades as the corporate infrastructure as well as mimicking many of the weaker security controls deployed within the home wireless environment. Penetration test on Wi-Fi networks can be performed in different ways. The main difference between these methods of conducting the tests is the amount of the knowledge of the implementation information or data made available to the penetration tester. Thus, penetration test conduct on Wi-Fi networks are categorized mainly into three, they are;

Black Box Test: this form of Wi-Fi penetration test assumes the penetration tester possess no prior knowledge of the Wi-Fi network to be tested other than the mere details such as the name of the client Wi-Fi network connection. The penetration tester is supposed to act a potential attacker who must gather information that is publicly available about the client's Wi-Fi network connection, such as domain and IP information.

White Box Test: Unlike the black box test type, white box test is vice versa. It simply implies the tester is been provided with complete knowledge and precise details about the Wi-Fi network infrastructure to be tested, such as encryption code and the IP address information.

The relative merits of these approaches are debatable. It is argued that black box testing most closely simulates the actions of a real hacker, however this ignores the fact that any targeted attack on a system most probably requires some knowledge of the system, and any inside attacker would be in possession of as much information as the system owners. In most cases it is preferable to assume a worst-case scenario and provide the testers with as much information as they require, assuming that any determined attacker would already have acquired these. Despite the full disclosure of information and knowledge by the client to the penetration tester, a white box form of penetration test, the gathering of information about the Wi-Fi network other than that given to the Pen Tester is still a relevant activity. This is solely because some Wi-Fi users, both private and corporate users are not aware, where their networks begin or end. Different sophisticated Wi-Fi network penetration tools, software and hardware are readily available in the IT market today. Software ranges from the netstumbler, Airsnort, CoreImpact Pro, are made available free on the web for attackers for activities such as WEP and WPA cracking and sniffing. Hardware tools such as the portable penetrator PP3000 PP6000 PP9000, WI-FI cards and Antennas amongst many others are also major tools available for Wi-Fi penetration test.

Penetration testing can be an invaluable technique to any Wi-Fi user's information security program. Basic white box penetration testing is often done as a fully automated inexpensive process. However, black box penetration testing is a labour-intensive activity and requires expertise to minimize the risk to targeted systems. At a minimum, it may slow the organization's networks response time due to network scanning and vulnerability scanning. Furthermore, the possibility exists that systems may be damaged in the course of penetration testing and may be rendered inoperable, even though the organization benefits in knowing that an intruder could have rendered the system inoperable. Although this risk is mitigated by the use of experienced penetration testers, it can never be fully eliminated.

METHODOLOGIES

Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing security tests and metrics. OSSTMM is a manual on security testing and analysis created by Pete Herzog, and provided by ISECOM, the non-profit Institute for Security and OpenMethodologies. The methodology itself that covers what, when, and where to test is free to use and distribute under the Open Methodology License (OML). The OSSTMM test cases are divided into five channels which collectively test: information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunication networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases. The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test, and how to measure the results. OSSTMM is also known for its rules of engagement, which define for both the tester and the client how the test needs to properly run starting from denying false advertising from testers to how the client can expect to receive the report. New tests for international best practices, laws, regulations, and ethical concerns are regularly added and updated. National Institute of Standards and Technology (NIST) NIST's methodology is less comprehensive than the OSSTMM; however, it is more likely to be accepted by regulatory agencies. For this reason, NIST refers to the OSSTMM. The Information Systems Security Assessment Framework (ISSAF) is a peer reviewed structured framework from the Open Information Systems Security Group that categorizes information system security assessment into various domains and details specific evaluation or testing criteria for each of these domains. It aims to provide field inputs on security assessment that reflect real life scenarios. The ISSAF should primarily be used to fulfil an organization's security assessment requirements and may additionally be used, as a reference for meeting other information security needs. It includes the crucial facet of security processes and, their assessment and hardening to get a complete picture of the vulnerabilities that might exist. The ISSAF, however, is still in its infancy.

Legal Ethics Involved in Penetration Testing

Wi-Fi users, both corporate and private are aware of the fact that conducting a penetration test on their Wi-Fi network would involve them revealing vital and sensitive information about their organization or personal data, for this reason they are sceptical recruiting a black hat (camouflage penetration tester that with malicious intent) hacker and also compelling to all the organizations employees to adhere to the organization ethical code. A few governmental and professional certifications have been set in to guaranty the worthiness and trust of a penetration testerto the conformance to the industry's practice.

The Council of registered ethical security testers (CREST) offers three certifications: CREST Registered Tester, CREST Certified Tester (Infrastructure) and CREST Certified Tester (Web Applications). The Information assurance certification review board (IACRB) manages a penetration testing certification known as the Certified Penetration Tester

(CPT). The CPT requires that the exam candidate pass a traditional multiple choice exam, as well as pass a practical exam that requires the candidate to perform a penetration test against live servers.

The International Council of E-Commerce consultants (EC-Council) certify individuals in various e-business and information security skills. These include the Certified Ethical Hacker course, Computer Hacking Forensics Investigator program, Licensed Penetration Tester program and various other programs, which are widely available worldwide. The EC-Council Network Security Administrator (ENSA) training was recognized at the 12th Colloquium for Information Systems Security Education (CISSE) when it was certified as meeting the Committee on national security system (CNSS) National Training Standard for Information Systems Security (INFOSEC) Professionals. SANS provides a wide range of computer security training arena leading to a number of SANS qualifications. In 1999, SANS founded GIAC, the Global Information Assurance Certification, which according to SANS has been undertaken by over 20,000 members to date. Two of the GIAC certifications are penetration testing specific: the GIAC Certified Penetration Tester (GPEN) certification; and the GIAC Web Application Penetration Tester (GWAPT) certification.

CONCLUSIONS

A private Penetration Test conduct on a sample Wi-Fi network access did prompt many security concerns. Private home Wi-Fi users seem not to be bothered about how secure their Wi-Fi network access is. Most of these users either seem to be nonchalant about the significance of securing their Wi-Fi network access or they are completely ignorant about properly securing their network access. Although the test conducted on the sample Wi-Fi network access was not a full professional test, with the use freely available online web penetration test tools it still showed how weak and porous the sample Wi-Fi network access security was. The tested Wi-Fi network access users were using the weakest known type of Wi-Fi network security mechanism "Wireless Equivalent Privacy" (WEP) even though they had the full option of properly securing their Wi-Fi network access with a better security specification standard. What most private home Wi-Fi network users fail to understand is the fact that, not properly using an enhanced security standard specification is the main and first passage for all potential attackers and hackers to gain unauthorized access into their Wi-Fi network. The response gathered from the administered question clearly shows that most the private home users do not take security issues seriously and are naïve of the implication of such an act. From the test being conducted on the sample private home Wi-Fi network, it clearly shows how ignorant most of these private home users are about their Wi-Fi network security. They seem to leave and trust the default security settings being put in place for their Wi-Fi network access by installation technicians after the first time the network device has been setup or installed. While most of these installation technicians are in a hurry to go setup other Wi-Fi network access device for other clients, they do not properly secure the security of the device routers for these users since it might take some time to do that and they have to meet up with other schedules they have for the day, thereby exposing their clients to malicious threats and attacks. Although most private home users also seem to neglect the fact that they should be solelyresponsible in ensuring that their Wi-Fi network access is well secured and protected against intruders who might gain unauthorized access into the Wi-Fi network access and use the opportunity to carry out illegal activities. There are numerous reason why private home Wi-Fi users should properly secure their network from public access, amongst these several reason are these important reasons;

- Private Home Wi-Fi network users tend to ignore the fact that not properly securing their Wi-Fi network access connection can grant an unauthorized access to intruders and these intruders can use their Internet connection for immoral, illegal and malicious activities. An authorized Internet user might carry out an illegal activity on the

users Internet connection such as the use and broadcast of pornographic materials, which might later be traced by law enforcement agents back to the network administrator and might cause some legal damage to the status of the Wi-Fi network owner.

- Also by not properly securing their Wi-Fi network connection access, they expose their network traffic to war drivers and attackers. These attackers or war drivers capture the Wi-Fi network traffic and examine them prior to the launch of their attack. During these network traffic capture, the speed and performance of the Wi-Fi network access is being drained and consumed i.e. man in the middle attack.
- Last but not the least, Private home Wi-Fi network users are ignorant of the fact that not properly securing their Wi-Fi network access exposes their network facilities and resources to illegal unauthorized users and attackers. These authorized users can get hold of sensitive data and information such as important passwords keys or financial data of the Wi-Fi network users and use them to carry out illegal activities that might cause network considerate loss.

The question being raised now is who or what outfit should be in charge of providing appropriate orientation about the significance of properly securing the private home use of Wi-Fi network connection access and also educating the users about various countermeasures that can be put in place against potential attacks. Since most private users do not consider frequent security audits or penetration test on their Wi-Fi network as a priority since most of them consider carrying out such task as being expensive, maybe the government should enforce a law on every home use Wi-Fi network user and also Wi-Fi network vendors to properly secure their network access or be fined by the law. In some part of the world today, some countries have already set this law into practice. Although no Wi-Fi network connection is 100% secure and free from malicious attacks, the following are the list of countermeasures private home Wi-Fi network users can employ from time to time to secure their Wi-Fi network access from intruders and attacks;

- Most Private home users do not turn of their network even when not in use, they leave it on and thereby allow potential intruders within their vicinity to discover and capture their network traffic prior to attack. Whenever the Wi-Fi network connection is not in use, it should be turned off. This measure is really effective because it impossible for an attacker to carry out any malicious intrusion activity on the network without the network on.
- Another common mistake most private home Wi-Fi users do make is not changing the default setting on their device router after installation. This allows attackers to hijack their network and thereby causing a denial of service (DOS) attack. Most Internet users are provided with the default username and password to every router, so therefore it is highly recommended that the default setting such as the username and password of the router should be change immediately after installation.
- Another very simple and effective countermeasure that can be employed by private home Wi-Fi users is for them to disable their Wi-Fi network SSID broadcast i.e. Wi-Fi network name. This measure can be done during the Wi-Fi setup mode in the device router settings by simply disabling the SSID broadcast. This will help in protect the network users against attackers sniffing the network traffic. Although this is only effective against intruders who are beginners and use common traffic sniffing tools.

- A very good and effective countermeasure against intruders and attacks is the MAC Address filtering. This feature is readily available on most device routers, this feature grants the Wi-Fi network administrator i.e. user (s) in granting the Wi-Fi connection access to specific Mac addresses only.
- Finally the most common and inexpensive countermeasure known to most private home users is the encryption method. Although it is a good method of securing one's Wi-Fi network connection access, but most private users do not select the best security specification standard available for them tosecure their Wi-Fi network; some even leave their network access open i.e. unsecured. Private home Wi-Fi users are therefore advised to use either the WPA or WPA2 security specification standard to secure their network, since it is being acclaimed to be a better way of securing Wi-Fi networks. Also the use of long and unfamiliar password keys would serve as a good choice.

REFERENCES

1. Karnik, A. & Passerini, K. (2005). Wireless Network Security. A Discussion from a Business Perspective. Wireless Telecommunications Symposium. 6th -7th April 2005. p. 261 – 267.
2. Corsaire. (2010). Penetration Testing Guide. [Online]. Available from: http://www.penetration-testing.com/ [Accessed: 11 March 2014]
3. SANS Institute. (2003). The Evolution of Wireless Security in 802.11 Networks: WEP, WPA, 802.11 Standards. Maryland: SANS Institute.
4. Mishra, A. et al. (2004). Security Issues in IEEE 802.11 Wireless Local- Area Networks: A Survey. Wireless Communications and Mobile Computing Journal. Vol. 4. (8). p. 821-833
5. Altunbasak, H. & Owen, H. (2004). Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LAN. 26th -29th Mar 2004. Southeast Conference.
6. Gast, M. (2005). 802.11 Wireless Networks: Definitive Guide. 2nd Edition. Sebastopol. O'Reilly Media Inc
7. Lavert, D. (2009). WPA vs. WPA2 (802.11i): How your Choice Affects your Wireless Network Security. [Online]. Available from: http://www.openxtra.co.uk/articles/wpa-vs-wep.
8. ISECOM. (n.d). Open Source Security Testing Methodology Manual. [Online]. Available from: http://www.isecom.org/osstmm/ [Accessed: 11 June 2010.
9. Walker, R, J. (2000). Unsafe at any key size; An analysis of the WEP Encapsulation. [Online]. October 2000. Available from: http://www.dis.org/wl/pdf/unsafe.pdf. [Accessed from: 4th July 2010.
10. PCI Security Standard Council. (2008). Information Supplement: Penetration Testing. [Online]. March 2008. Available from: https://www.pcisecuritystandards.org/minisite/en/docs/informationsupplement.pdf. [Accessed from: 6th July 2010.
11. Farrow, R. (2003).The value of penetration testing. [Online].March 2003. Available from: http://www.spirit.com/Network/net0303.html [Accessed 6th July 2010]
12. Moscowitz, R. (2003). Weakness in Passphrase Choice in WPA Interface. WNN Wi-Fi Net News. [Online]. 4th November. Available from: http://wifinetnews.com/archives/002452.html. [Accessed: 6th July 2010]

13. Borisov, N. et al. (2001). Intercepting Mobile Communications: The Insecurity of 802.11. [Online]. July 2001. Available from: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

14. Borisov, N. et al. (2001). Intercepting Mobile Communications: The Insecurity of 802.11. [Online]. July 2001. Available from: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

15. Peterson, L. & Davie, S. (2003). Computer Networks: A Systems Approach. 3rd Edition. CA, U.S.A. Morgan Kaufmann Publishers.

16. McClure, S. et al. (2004). Hacking Exposed: Network Security secrets and solutions. 4th Edition. NY, U.S.A. McGraw.

17. Stallings, W. (2003). Cryptography and Network Security: Principles and Practice. 3rd Edition. NJ, U.S.A. Prentice Hall

18. Welch, D. & Lathrop, S. (2003). Wireless Security Taxonomy: Proceedings of the IEEE Workshop On information assurance. United State Military Academy, West Point, New York. June 2003

19. Sankar, K et al. (2003). Cisco Wireless LAN Security: Expert Guidance for securing your 802.11 networks. U.S.A. Cisco Press.

20. IASTED. (2004). International Association of Science and Technology for Development. [Online]. Available from: http://www.iasted.com/conferences/2004/banff/WNET-Hunt3b.pdf. [Accessed: 7th June 2010]

21. Edgar, S. L. (2003). Morality and Machines. 2nd Edition. Sudbury, MA. Jones and Bartlett Publishers

22. P fleeger, P. et al. (2003). Security in computing. 3rd Edition. Upper Saddle River, NJ. Prentice Hall.

23. Internet Security System. (2001). Penetration Tests: Baseline for effective Information Protection. [Online]. Available from: http://www.iss.net/documents/whitepapers/pentestwp.pdf. [Accessed: 11th June 2010].

24. Seymour, B. & Kabay, M. (2002). Computer Security Handbook. 4th Edition. Indianapolis, India, USA. John Wiley & Sons.

25. SAP Penetration Testing. Croce, M. (2009). Black Hat Europe 09 Briefing and Training. [Online Video]. April 16th. Available From: http://www.securitytube.net/SAP-PenetrationTesting-(Blackhat-2009)-video.aspx. [Accessed: April 12th 2014]

26. United States. Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology. (2003). Guideline on Network Security Testing: Recommendationsof the National Institute of Standards and Technology. Gaithersburg: NIST Special Publication 800-42.

27. INSOMNIA. (2008). Increasing the Value of penetration testing. [Online]. Available From: http://www.insomniasec.com/publications/Increasing_The_Value_Of_Penetration_Testingwp.pdf. [Accessed: 8th March 2010]

28. Coleman, D. & Westcott, D. (2009). CWNA®: Certified Wireless Network Administrator Official Study Guide. Sybex.

29. Klevinsky, T. J. et al. (2002). Hack I.T. - Security through Penetration Testing. Indianapolis, Indiana. Addison- Wesley Professional.

30. Wilhelm, T. (2010). Professional Penetration Testing: Creating and operating a formal hacking lab. USA, Burlington. Syngress.